IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA Plaintiff,	§ §	
v.	§ §	NO: 6:25-CV-00052
$271,623.93 IN UNITED STATES CURRENCY Defendant.	§ § §	

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed since September 2001. My current position is the Resident Agent in Charge (RAIC) of the USSS Tyler Resident Office. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law

enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

a. $271,623.93 in Lead Bank account XXXXXX3142

("TARGET ACCOUNT" or "Defendant Property");

contained in the form of Check No. 072972 and was seized on or about November 25, 2024, in Tyler, Texas.

LEGAL AUTHORITY FOR FORFEITURE

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S.

based victims, to include victims located in the Eastern District of Texas. Scammers then fooled victims into "investing" in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims' money.

5. This type of scam is often identified as a cryptocurrency investment fraud scheme and involves scammers spending significant time getting to know, targeting and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH or USDC deposit address, and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim's account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve a large portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or

traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the "placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the "integration" phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to wire fraud in violation of 18 U.S.C. § 1343 or a conspiracy to commit wire fraud, as set forth in 18 U.S.C. § 1349. Wire fraud is an SUA.

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or 1349 is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept.

FACTS SUPPORTING FORFEITURE

14. The United States is investigating a cryptocurrency investment fraud scheme that utilizes spoofed domains as part of their fraudulent network to lure and trick unsuspecting victims. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from these victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of these victims. The Elights Trading Inc. bank account was provided to victims located within the Eastern District of Texas as a means in which they would pay their "taxes and/or fees" concerning their "earnings" as part of this scheme.

16. Investigators interviewed multiple victims who sent funds to the Citibank account held in the name of Elights Trading. In summary, these victims reported to have been tricked into believing they were investing in cryptocurrency, when in fact they were provided with links or information leading them to use spoofed domains or applications of legitimate cryptocurrency exchanges. One of these victims was identified as T.G.

Victim T.G.

17. Investigators interviewed victim T.G. regarding the $230,000 transaction remitted to the Elights Trading Account. T.G. met a person purporting to be a friend on

Facebook in or about May 2023, but has never met this individual face to face. T.G.'s new female friend portrayed herself as being very wealthy and T.G. inquired how he could invest money to earn a large and safe return. T.G.'s friend provided a link to Telegram where he was led to believe he was working with employees of OKEX, a cryptocurrency exchange. T.G. received instructions via Telegram regarding investments, including the information for the Elights Trading account. T.G. stated he believed he was purchasing options in cryptocurrency and not specific cryptocurrency coins such as BTC. T.G. has invested approximately $850,000 in total by sending to other bank accounts he received from the OKEX Telegram communications. T.G. stated he has only requested small withdrawals from his investment and has received only a few thousand dollars and has not made any large withdrawal requests.

18. T.G. informed USSS investigators that during this scheme, he was provided the JPMC Bank account in the name of Sunshines Trading, account number ending in 2181. A review of JPMC Bank records pertaining to this account reflect T.G. sent $80,000 to this account on September 20, 2023.

Victim B.H.

19. USSS investigators interviewed victim B.H. regarding the $80,000.00 transaction he sent to the JPMC account in the name of Sunshines Trading, account number ending in 8678. B.H. was victimized by this cryptocurrency investment scheme, and it all began by meeting a person on Facebook who used the name Mona Johnson Chen. Chen introduced B.H. to the OKEX platform, the same platform introduced to victim T.G. mentioned earlier in this affidavit. B.H. suffered a loss of approximately

$352,000.00 as a result of this scheme to the following entities: Sunshines Trading, Royal Chronos Limited, and Bluewave Trade Limited. B.H. recently attempted to withdraw his funds from OKEX, but was informed he would need to pay $19,000 in taxes and/or fees prior to receiving his funds.

Victim A.V.V.

20. USSS investigators interviewed victim A.V.V. regarding the $55,750.00 transaction she sent to the JPMC account in the name of Sunshines Trading, account number ending in 2181. A.V.V. stated she was contacted by an individual via LinkedIn using the name Toby Li, who stated he worked for Apple and was impressed with A.V.V.'s qualifications. A.V.V. stated Toby Li eventually convinced A.V.V. into investing in cryptocurrency by funding a crypto.com account and sending funds to a wallet A.V.V. was made to believe existed at Blackcoin.com. A.V.V. provided transaction details of the funds she sent as part of this scheme, which included $17,000 on July 28, 2023 to Stone Water Trading account ending in 1823 and $20,000 on October 16, 2023 to another identified account. A.V.V. stated she has not been able to retrieve her funds as she was promised. A.V.V. stated she has suffered a great financial loss of approximately $300,000.00 because of this scheme.

INVESTIGATION IDENTIFIES ADDITIONAL VICTIMS WHO SENT FUNDS TO STONE WATER TRADING

Victim T.K.

21. USSS investigators identified and interviewed victim T.K. regarding the $10,000 he sent to a suspect account that was previously seized in this investigation

pursuant to a search and seizure warrant. T.K. stated he received a wrong number call from an unknown female subject on or about August 3, 2023. T.K. stated the unknown female caller befriended him, and they communicated often. T.K. stated their conversations turned to investments and how to make money by investing in Gold via "Goldman Sachs." T.K. stated he sent various wire transfers to bank accounts provided by the female and claimed he was able to make small cash withdrawals early on in the scheme. T.K. stated he was persuaded to invest additional funds. When he attempted to make larger withdrawals from his "investment account", he was informed he needed to pay fees equal to 10% of his "earnings." T.K. stated he paid the 10% fee and an additional 15% fee to separate entities, and still was unable to withdraw any of his funds.

22. T.K. stated in addition to a previously seized account in this investigation, he also sent payments to the JPMC bank account of Stone Water Trading as noted below:

9/5/23	$6,823.58	Stone Water Trading LLC/JPMC
9/11/23	$5,000.00	Stone Water Trading LLC/JPMC

23. USSS investigators obtained Internet Crime Complain Center (hereafter known as IC3) reports regarding queries related to Stone Water Trading. There were thirteen reports by separate victims whose transactions totaled $622,568.00. A review of JPMC bank records regarding Stone Water Trading's bank account verified these deposits as reflected in these IC3 reports. These victims all reported similar instances as other victims who were previously interviewed by USSS investigators throughout this investigation.

24. Furthermore, during the time period of September 1 through 29, 2023, the JPMC account of Stone Water Trading, account number ending in 1823, received approximately $6,458,478.87 in deposits, which originated mostly from victims of the cryptocurrency investment fraud scheme or transactions from other reported shell companies that also received victim funds of the same fraud scheme. During this time frame, the JPMC Stone Water Trading account ending in 1823 sent three wire transactions to the TARGET ACCOUNT totaling approximately $1,323,408.

25. On November 30, 2023, a federal seizure warrant (6:23-MJ-270) was issued in the Eastern District of Texas for the JPMC account in the name of Stone Water Trading, as it was determined to hold proceeds of the cryptocurrency investment fraud scheme.

SUNSHINES TRADING ACCOUNTS RECEIVED FRAUD PROCEEDS

26. Investigators issued a federal grand jury subpoena to JPMC and obtained the bank records for the JPMC Bank accounts in the name of Sunshines Trading Inc., account number ending in 2181; account number ending in 8678; and the account held in the name of Qi Sun account number ending in 7330. These bank records identified the signor on accounts 2181 and 8678 as Qi Sun. The records indicate that on or about August 9, 2023, Qi Sun opened the business bank accounts identifying Sunshines Trading Inc. as a corporation. The records reflect that Sun provided the business address of 2124 Las Lomitas Drive, Hacienda Heights, California 91745.

27. USSS investigators identified and interviewed multiple individuals who wire transferred monies to the identified accounts in the name of Sunshines Trading and

Qi Sun. These individuals reported to have been victimized by a cryptocurrency fraud scheme as they were unable to recover any significant portions of their reported investments. As a result, a federal seizure warrant (6:23-MJ-259) was obtained in the Eastern District of Texas for the aforementioned accounts on November 2, 2023.

28. On April 3, 2024, a federal grand jury in the Middle District of Tennessee returned an indictment (3:24-00073) against Qi Sun for violations pertaining to the cryptocurrency investment fraud scheme, including violations of 18 USC §§ 1343 and 1349.

INVESTIGATION OF ROYAL CHRONOS LIMITED

29. USSS investigators initiated an investigation of Royal Chronos Limited (RCL) which held bank accounts at JPMC Bank. USSS investigators learned from JPMC employees that RCL operated bank accounts ending in 3726 and 2357 that were recently closed by JPMC. However, RCL was allowed to establish a new account at JPMC Bank.

30. USSS investigators obtained IC3 reports regarding queries related to RCL. There were two reports by separate victims whose recent transactions totaled $183,000.00. A review of JPMC bank records in the name of RCL verified that these deposits were reflected in the IC3 reports. These victims all reported similar incidents as the other victims who were interviewed by USSS investigators during this investigation.

31. The JPMC accounts held in the name of Royal Chronos Limited and other closely related accounts were identified during this investigation as accounts that received wire transactions from victims of this cryptocurrency investment fraud scheme. As a result, a federal seizure warrant (6:24-MJ-5) was obtained in the Eastern District of

Texas on January 17, 2024, for the JPMC accounts held in the name of Royal Chronos Limited and other related accounts.

PROCEEDS FROM SUNSHINES TRADING, STONE WATER TRADING, AND ROYAL CHRONOS LIMITED ARE TRANSFERRED TO THE TARGET ACCOUNT

32. USSS investigators reviewed bank records pertaining to the accounts of Royal Chronos Limited, Sunshines Trading, Stone Water Trading, Qi Sun, and others, and discovered proceeds from these accounts were being funneled to the TARGET ACCOUNT.

33. USSS investigators obtained the bank records pertaining to the TARGET ACCOUNT via grand jury subpoena. The records indicated the TARGET ACCOUNT was opened on or about July 21, 2023 with a $100,000 deposit from a Bankprov bank account. The account opening documents indicate an individual using the name Aiju Xie is the sole owner/shareholder of Paretone Capital LTD. A document titled as the Certificate of Incumbency, notes that Xie is a shareholder, and Wei Wang is the director of the company. A document titled LLC Authorization Resolution notes that the following persons are authorized to act on behalf of Paretone Capital LTD: Gaoyuan Bi, Shenshuai Chen, and Wei Wang. A copy of the company's bylaws was also included, which reflect that Gaoyuan Bi is a Partner/Chief Compliance and the address of 97 E. Brokaw Road, San Jose, California 95112 was used by Xie and Paretone.

34. Paretone Capital purports to operate a money services business, exchanging fiat currency for cryptocurrency and/or cryptocurrency for fiat currency. A grand jury subpoena served to Paretone Capital indicates they provide cryptocurrency purchase

agreements to their clients, such as Stone Water Trading, which verifies that Paretone Capital operates as a money services business.

35. The account statements for the TARGET ACCOUNT reveal a significant amount of wire transactions originating from several entities known to this investigation, including Royal Chronos Limited, Sunshines Trading, Stone Water Trading, and Qi Sun.

36. Specifically, in reviewing the bank records for the TARGET ACCOUNT for the month of August 2023, Royal Chronos Limited sent the TARGET ACCOUNT $154,800 on August 29, 2023. On August 30, 2023, Sunshines Trading sent the TARGET ACCOUNT $147,340. That same day, Qi Sun sent the TARGET ACCOUNT $28,320. These funds were derived from entities identified in this investigation to have received the proceeds of the cryptocurrency investment fraud scheme identified herein.

37. Furthermore, a review of the bank statement for the TARGET ACCOUNT dated September 1 through 29, 2023, indicates the beginning balance was $1,374,086.24 and an ending balance of $258,549.84. The total deposits into the TARGET ACCOUNT during this time frame were $8,448,149.00 and the total withdrawals amounted to $9,563,685.40. During this time period, the records indicate five (5) transactions were received by the TARGET ACCOUNT from Royal Chronos Limited totaling $945,493; eleven (11) transactions were received by the TARGET ACCOUNT from Sunshines Trading totaling $1,694,770; three (3) transactions were received by the TARGET ACCOUNT from Stone Water Trading totaling $1,323,408; and one (1) transaction was received by the TARGET ACCOUNT from Qi Sun for $28,600. The most significant withdrawals during this time frame included transactions to a separate account in the

name of Paretone Capital ($2,005,00.00); Galaxy Digital Trading Cayman LLC ($3,550,000.00) and Yellowstone Trade Limited ($350,000.00).[1]

38. The bank statements pertaining to the TARGET ACCOUNT during the time period of October 1 through 31, 2023, included a beginning balance of $258,549.84 and deposits totaling approximately $1,221,220.64. These deposits were sent from an entity identified as U Fintech Hub Inc. The significant withdrawals during this time period reflect payments to a separate account held in the name of Paretone Capital ($700,000.00) and to other private individuals (approximately $532,000.00). The ending balance in October 2023 for the TARGET ACCOUNT was $135,234.84.

39. There were also additional entities that sent funds to the TARGET ACCOUNT that have been identified in other investigations known to me, to include BQRIG Inc, Stillman Digital LLC, and KRG Trading Inc. These entities and their related bank accounts have received proceeds of the cryptocurrency investment fraud scheme.

40. On November 1, 2023, USSS investigators issued a voluntary freeze request to Lead Bank in an effort to restrain the remaining assets in the TARGET ACCOUNT. Since the time the freeze was requested, the TARGET ACCOUNT was voluntarily restrained by Lead Bank. However, a deposit of $138,000 was received on November 2, 2023, from U Fintech Hub.

[1] Yellowstone Trade Limited is an entity registered in Hong Kong that was established by Wei Wang, who is a partner in Paretone Capital LTD. The bank accounts of Yellowstone Trade Limited are known to have received fraud proceeds from other identified shell companies in this investigation.

INVESTIGATION OF U FINTECH HUB

41. USSS investigators identified U Fintech Hub as a money transmitting business that is registered in the state of California. U Fintech Hub utilized a bank account at Coastal Community bank to conduct transactions with the TARGET ACCOUNT. The funds that were deposited into U Fintech's account from August 1 through October 31, 2023 were derived from unknown sources to include Stripe, Inc. and Bluevine. Based on my experience conducting money laundering investigations, I know individuals used both Stripe, Inc. and Bluevine to launder proceeds of specified unlawful activities such as those described herein.

42. This investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

CONCLUSION

43. I submit that this affidavit supports probable cause to forfeit all funds, monies, and other things of value up to $271,623.93 from Lead Bank account XXXXXX3142.

44. Based on my experience and the information herein, I have probable cause to believe that the seized $271,623.93 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to money laundering transactions, and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

45. I also have probable cause to believe that the seized $271,623.93 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Brad Schley, Special Agent
U.S. Secret Service